



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/663,178	09/15/2003	Harlan T. Beverly	P14504	2832
46915	7590	10/11/2006	EXAMINER HA, LEYNNA A	
KONRAD RAYNES & VICTOR, LLP. ATTN: INT77 315 SOUTH BEVERLY DRIVE, SUITE 210 BEVERLY HILLS, CA 90212			ART UNIT 2135	PAPER NUMBER

DATE MAILED: 10/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/663,178	BEVERLY, HARLAN T.
	Examiner	Art Unit
	LEYNNA T. HA	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on ____.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-34 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) Claim(s) ____ is/are allowed.
- 6) Claim(s) 1-34 is/are rejected.
- 7) Claim(s) ____ is/are objected to.
- 8) Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 20 July 2006 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. ____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. ____. |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>6/22/04</u> . | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

1. Claims 1-34 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. **Claims 1-34 are rejected under 35 U.S.C. 102(e) as being anticipated by Pinkerton, et al. (US 7,007,103).**

As per claim 1:

Pinkerton discloses a method for processing data packets sent through a network, comprising:

receiving data packets from a host through the network wherein the received packets were, prior to receipt, encrypted and fragmented after encryption; (**col.1, lines 50-55 and col.11, lines 41-44**)

reassembling the fragmented packets using a communication protocol offload engine in a network adaptor coupling a host central processing unit to the network; (**col.12, lines 20-25 and col.18, lines 15-21**)

Art Unit: 2135

decrypting the reassembled packets of encryption using a security offload engine in the network adaptor; and (**col.6, lines 40-44 and col.20, lines 54-55**)

forwarding the decrypted and reassembled packets to the communication protocol offload engine. (**col.20, lines 55-57**)

As per claim 2: See **col.18, lines 15-21 and col.20, lines 54-57**; discusses the method of claim 1 further comprising: receiving from a remote host through the network additional packets which were encrypted in a first encryption, fragmented after the first encryption and encrypted in a second encryption after the fragmentation; decrypting the fragmented packets of the second encryption of using the security offload engine; reassembling the fragmented packets decrypted of the second encryption using a communication protocol offload engine; decrypting the reassembled packets of the first encryption using the security offload engine; and forwarding the decrypted and reassembled additional packets to the communication protocol offload engine.

As per claim 3: See **col.9, lines 45-51 and col.18, lines 15-21**; discusses the method of claim 1, further comprising: receiving from a remote host through the network additional packets which were encrypted and fragmented after all encryption; reassembling the fragmented additional packets using the communication protocol offload engine; decrypting the reassembled additional packets of encryption using the security offload engine; and forwarding the decrypted and reassembled additional packets to the communication protocol offload engine.

As per claim 4: See **col.18, lines 15-30 and col.20, lines 54-57**; discusses the method of claim 1, further comprising: receiving from a remote host through the network additional packets which were fragmented and then encrypted; decrypting the fragmented additional packets of encryption using the security offload engine; and reassembling the fragmented and decrypted additional packets using the communication protocol offload engine.

As per claim 5: See col.11, lines 41-44; discusses the method of claim 1, further comprising: receiving from a remote host through the network additional packets which were fragmented but not encrypted; reassembling the fragmented and unencrypted packets using the communication protocol offload engine.

As per claim 6: See col.1, lines 50-55 and col.9, lines 45-48; discusses the method of claim 1, further comprising: receiving from a remote host through the network additional packets which were encrypted but not fragmented; decrypting the unfragmented packets of encryption using the security offload engine; and forwarding the decrypted additional packets to the communication protocol offload engine.

As per claim 7: See col.2, lines 12-16 and 49-63; discusses the method of claim 2, wherein the first encryption is a transport mode encryption and the second encryption is a tunnel mode encryption.

As per claim 8: See col.11, lines 41-44 and col.20, lines 47-51; discusses the method of claim 1, further comprising: feeding the received packets through a feedforward path from a network interface receiver in the network adaptor, through the security offload engine and to the communication protocol offload engine to be reassembled; and feeding the reassembled packets from the communication protocol offload engine through a feedback path from the communication protocol offload engine to the security offload engine to be decrypted.

As per claim 9: See col.18, lines 15-21 and col.20, lines 54-57 ; discusses the method of claim 8, wherein said forwarding comprises: feeding the decrypted and reassembled packets through the feedforward path from the security offload engine to the communication protocol offload engine; said method further comprising: extracting a data payload from the decrypted and reassembled packets using the communication protocol offload engine.

As per claim 10: See col.6, lines 40-44 and col.20, lines 47-51; discusses the method of

claim 8, further comprising: multiplexing a flow of data packets in the feedforward path from the network interface receiver to the security offload engine and a flow of data packets in the feedback path from the communication protocol offload engine to the security offload engine.

As per claim 11:

Pinkerton discloses a network adaptor for use with a network, comprising:
a security offload engine having an input and an output and adapted to decrypt encrypted packets; (**col.1, lines 50-55**)
a communication protocol offload engine having an input and an output and adapted to reassemble fragmented packets; (**col.2, lines 12-16 and 49-63**)
a network interface receiver having an output coupled to the security offload engine input and an input adapted to receive from the network packets which were, prior to receipt, encrypted and fragmented after encryption; (**col.6, lines 40-44 and col.12, lines 20-25**)
a feedforward path coupling said receiver output to said security offload engine input and said security offload engine output to said communication protocol offload engine input; (**col.11, lines 41-44**)
a feedback path coupling said communication protocol offload engine output to said security offload engine input; and (**col.2, lines 50-65 and col.20, lines 47-51**)
logic adapted to feed the fragmented packets from the network interface receiver through the feedforward path to the communication protocol offload engine to be reassembled in the communication protocol offload engine, to feed the reassembled packets from the communication protocol offload engine through the feedback path to the security offload engine to be decrypted in the security offload engine, and to feed the decrypted and reassembled packets from the security offload engine, through the feedforward path to the communication protocol offload engine. (**col.18, lines 15-21 and col.20, lines 55-57**)

As per claim 12: See col.18, lines 15-21 and col.20, lines 24-57; discusses the adaptor of claim 11: wherein said receiver is adapted to receive from the network additional packets which were encrypted in a first encryption, fragmented after the first encryption and encrypted in a second encryption after the fragmentation; and wherein the logic is adapted to feed the fragmented packets of the second encryption from the network interface receiver through the feedforward path to the security offload engine to be decrypted of the second encryption in the security offload engine; to feed the fragmented packets decrypted of the second encryption from the security offload engine through the feedforward path to the communication protocol offload engine to be reassembled in the communication protocol offload engine, to feed the reassembled packets of the first encryption from the communication protocol offload engine through the feedback path to the security offload engine to be decrypted of the first encryption in the security offload engine, and to feed the decrypted and reassembled additional packets packets from the security offload engine, through the feedforward path to the communication protocol offload engine.

As per claim 13: See col.18, lines 15-21 and col.20, lines 55-57; discusses a adaptor of claim 11: wherein said receiver is adapted to receive from the network additional packets which were encrypted and fragmented after all encryption; and wherein the logic is adapted to feed the fragmented additional packets from the network interface receiver through the feedforward path to the communication protocol offload engine to be reassembled in the communication protocol offload engine, to feed the reassembled additional packets from the communication protocol offload engine through the feedback path to the security offload engine to be decrypted in the security offload engine, and to feed the decrypted and reassembled additional packets packets from the security offload engine, through the feedforward path to the communication protocol offload engine.

As per claim 14: See col.1, lines 50-55 and col.20, lines 24-57; discusses the adaptor of claim 11: wherein said receiver is adapted to receive from the network additional packets which were fragmented and then encrypted; and wherein the logic is adapted to feed the fragmented additional packets from the network interface receiver through the feedforward path to the security offload engine to be decrypted in the security offload engine, and to feed the decrypted additional packets from the security offload engine, through the feedforward path to the communication protocol offload engine.

As per claim 15: See col.11, lines 41-44 and col.20, lines 47-51; discusses the adaptor of claim 11: wherein said receiver is adapted to receive from the network additional packets which were fragmented but not encrypted; and wherein the logic is adapted to feed the fragmented additional packets from the network interface receiver through the feedforward path to the communication protocol offload engine to be reassembled in the communication protocol offload engine.

As per claim 16: See col.11, lines 41-44 and col.20, lines 47-51; discusses the adaptor of claim 11: wherein said receiver is adapted to receive from the network additional packets which were encrypted but not fragmented; and wherein the logic is adapted to feed the encrypted additional packets from the network interface receiver through the feedforward path to the security offload engine to be decrypted of the encryption in the security offload engine, and to feed the decrypted and additional packets from the security offload engine, through the feedforward path to the communication protocol offload engine.

As per claim 17: See col.2, lines 12-16 and 49-63; discusses the adaptor of claim 12 wherein the first encryption is a transport mode encryption and the second encryption is a tunnel mode encryption.

As per claim 18: See col.18, lines 15-21 and col.20, lines 55-57; discusses the adaptor of

Art Unit: 2135

claim 111 the communication protocol offload engine is adapted to extracting a data payload from the decrypted and reassembled packets.

As per claim 19: See col.6, lines 40-44 and col.12, lines 20-25; discusses the adaptor of claim 11 wherein the feedback path and the feedforward path includes a multiplexor adapted to multiplex a flow of data packets in the feedforward path from the network interface receiver output to the security offload engine input and a flow of data packets in the feedback path from the communication protocol offload engine output to the security offload engine input.

As per claim 20: See col.18, lines 15-21 and col.20, lines 55-57; discusses the adaptor of claim 11 wherein the feedback path includes a buffer wherein said logic is adapted to store reassembled packets from the communication protocol offload engine to await multiplexing by said multiplexor to the security offload engine input.

As per claim 21:

Pinkerton discloses a system for use with a network, comprising:

a system memory; a processor coupled to the system memory; (**col.4, lines 25-35**)

data storage coupled to the processor and the system memory;

a data storage controller adapted to manage Input/Output (I/O) access to the data storage; (**col.5, lines 44-55**)

and a network adaptor which includes:

a security offload engine coupled to the memory and having an input and an output and adapted to decrypt encrypted packets; (**col.4, lines 50-57**)

a communication protocol offload engine having an input and an output and adapted to reassemble fragmented packets; (**col.1, lines 50-55 and col.2, lines 12-16**)

Art Unit: 2135

a network interface receiver having an output coupled to the security offload engine input and an input adapted to receive from the network packets which were, prior to receipt, encrypted and fragmented after encryption; (**col.6, lines 40-44 and col.11, lines 41-44**)

a feedforward path coupling said receiver output to said security offload engine input and said security offload engine output to said communication protocol offload engine input; (**col.2, lines 50-65 and col.20, lines 47-51**)

a feedback path coupling said communication protocol offload engine output to said security offload engine input; and (**col.1, lines 50-55 and col.2, lines 12-16**)

logic adapted to feed the fragmented packets from the network interface receiver through the feedforward path to the communication protocol offload engine to be reassembled in the communication protocol offload engine, to feed the reassembled packets from the communication protocol offload engine through the feedback path to the security offload engine to be decrypted in the security offload engine, and to feed the decrypted and reassembled packets from the security offload engine, through the feedforward path to the communication protocol offload engine. (**col.18, lines 15-21 and col.20, lines 55-57**)

As per claim 22:

Pinkerton discloses an article of manufacture for use with a network wherein the article of manufacture causes operations to be performed, the operations comprising:

receiving data packets from a remote host through the network wherein the received packets were, prior to receipt, encrypted and fragmented after encryption; (**col.1, lines 50-55 and col.11, lines 41-44**)

reassembling the fragmented packets using a communication protocol offload engine in a network adaptor coupling a host central processing unit to the network; (**col.18, lines 15-21**)

decrypting the reassembled packets of encryption using a security offload engine in the network adaptor; and **(col.2, lines 12-16 and 49-63)**

forwarding the decrypted and reassembled packets to the communication protocol offload engine. **(col.20, lines 55-57)**

As per claim 23: See col.18, lines 15-21 and col.20, lines 24-57; discusses the article of manufacture of claim 22, wherein the operations further comprise: receiving from a remote host through the network additional packets which were encrypted in a first encryption, fragmented after the first encryption and encrypted in a second encryption after the fragmentation; decrypting the fragmented packets of the second encryption of using the security offload engine; reassembling the fragmented packets decrypted of the second encryption using a communication protocol offload engine; decrypting the reassembled packets of the first encryption using the security offload engine; and forwarding the decrypted and reassembled additional packets to the communication protocol offload engine.

As per claim 24: See col.18, lines 15-21 and col.20, lines 24-57; discusses the article of manufacture of claim 22, wherein the operations further comprise: receiving from a remote host through the network additional packets which were encrypted and fragmented after all encryption; reassembling the fragmented additional packets using the communication protocol offload engine; decrypting the reassembled additional packets of encryption using the security offload engine; and forwarding the decrypted and reassembled additional packets to the communication protocol offload engine.

As per claim 25: See col.11, lines 41-44; discusses the article of manufacture of claim 22, wherein the operations further comprise: receiving from a remote host through the network additional packets which were fragmented and then encrypted; decrypting the fragmented additional packets of encryption using the security offload engine; and reassembling the

fragmented and decrypted additional packets using the communication protocol offload engine.

As per claim 26: See col.11, lines 41-44 and col.20, lines 47-51; discusses the article of manufacture of claim 22, wherein the operations further comprise: receiving from a remote host through the network additional packets which were fragmented but not encrypted; reassembling the fragmented and unencrypted packets using the communication protocol offload engine.

As per claim 27: See col.11, lines 41-44 and col.20, lines 47-51; discusses the article of manufacture of claim 22, wherein the operations further comprise: receiving from a remote host through the network additional packets which were encrypted but not fragmented; decrypting the unfragmented packets of encryption using the security offload engine; and forwarding the decrypted additional packets to the communication protocol offload engine.

As per claim 28: See col.2, lines 12-16 and 49-63; discusses the article of manufacture of claim 23, wherein the first encryption is a transport mode encryption and the second encryption is a tunnel mode encryption.

As per claim 29: See col.18, lines 15-21 and col.20, lines 55-57; discusses the article of manufacture of claim 22, wherein the operations further comprise: feeding the received packets through a feedforward path from a network interface receiver in the network adaptor, through the security offload engine and to the communication protocol offload engine to be reassembled; and feeding the reassembled packets from the communication protocol offload engine through a feedback path from the communication protocol offload engine to the security offload engine to be decrypted.

As per claim 30: See col.18, lines 15-21 and col.20, lines 55-57; discusses the article of manufacture of claim 29, wherein said forwarding operation comprises: feeding the decrypted and reassembled packets through the feedforward path from the security offload engine to the communication protocol offload engine; and wherein the operations further comprise extracting

a data payload from the decrypted and reassembled packets using the communication protocol offload engine.

As per claim 31: See col.6, lines 40-44 and col.12, lines 20-25;; discusses the article of manufacture of claim 22, wherein the operations further comprise: multiplexing a flow of data packets in the feedforward path from the network interface receiver to the security offload engine and a flow of data packets in the feedback path from the communication protocol offload engine to the security offload engine.

As per claim 32: See col.6, lines 40-44 and col.111, lines 40-44; discusses the system of claim 21, wherein the logic is further adapted to: multiplex a flow of data packets in the feedforward path from the network interface receiver to the security offload engine and a flow of data packets in the feedback path from the communication protocol offload engine to the security offload engine.

As per claim 33:

Pinkerton discloses a adaptor, comprising:

a network interface controller adapted to receive fragments of network packets, at least some of the fragments originating from network packets encrypted prior to fragmentation; (**col.4, lines 50-57 and col.6, lines 40-44**)

a communication protocol offload engine to reassemble the network packets from the received fragments; (**col.2, lines 12-16 and col.18, lines 15-21**)

a security offload engine to decrypt at least a portion of the reassembled network packets to provide decrypted packets; and (**col.4, lines 50-57**)

logic adapted to selectively return at least some of the decrypted packets to the communication protocol offload engine. (**col.20, lines 55-57**)

As per claim 34: See col.2, lines 12-16; discusses the adaptor of claim 33 wherein the

communication protocol of the communication protocol offload engine is the Transmission Control Protocol (TCP) and Internet Protocol (IP).

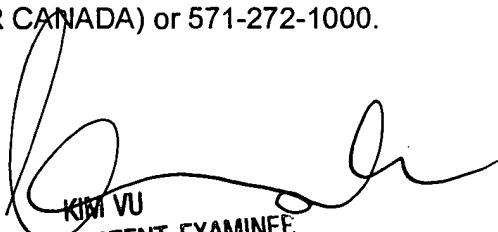
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100